Linux Security Best Practices with Fedora

Uditha Bandara Wijerathna
udinnet@fedoraproject.com

MAY 18-20, 2012

What is Computer Security?

- Covers a wide area of computing and information processing
- Several terms and metrics have entered our daily business vocabulary
- The availability and trustworthiness of data can be the difference between success and failure

Security Controls

Computer security is often divided into three distinct master categories, commonly referred to as *controls*

- Physical
- Technical
- Administrative

Security Controls Contd..

Physical control

Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.

- Closed-circuit surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)

Security Controls Contd..

Technical control

Technical controls use technology as a basis for controlling the access and usage of sensitive data
throughout a physical structure and over a network. Technical controls are far-reaching in scope and
encompass such technologies as

- Encryption
- Smart cards
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software

Security Controls Cont'd..

Administrative control

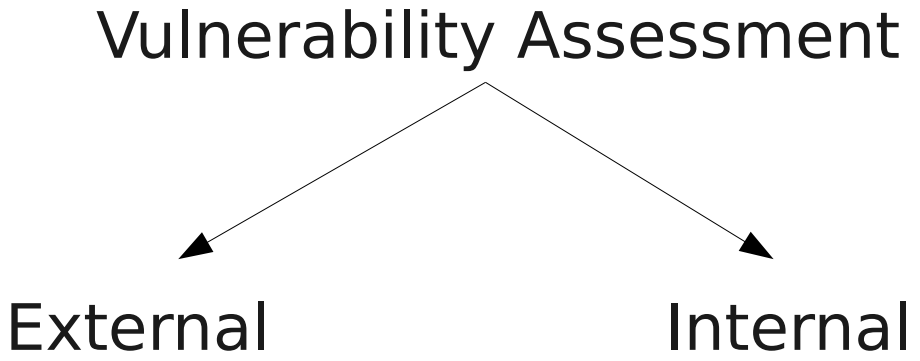
Administrative controls define the human factors of security. They involve all levels of personnel within an organization and determine which users have access to what resources and information by such means as

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting

Thinking Like the Enemy

- Given the complexity of today's software and networking environments, exploits and bugs are a certainty.
- you must think like a cracker and gauge the security of your systems by checking for weaknesses
- There can be potential issues that can be addressed before a cracker explores it.
- Think about your system's security by taking your home as an example.
- Focus on their tools,mentality, and motivations, and you can then react swiftly to their actions.

Defining Assessment and Testing



Benefits

- Creates proactive focus on information security
- Finds potential exploits before crackers find them
- Results in systems being kept up to date and patched
- Promotes growth and aids in developing staff expertise
- Reduce financial loss and negative publicity

Hacker and Cracker

Hacker...
Bad or Good?

Hacking Culture

MAY 18-20, 2012

Threats

Threats to

- Network Security
- Server Security
- Workstation and Home PC Security

Threats to Network Security

Insecure Architecture

A misconfigured network is a primary entry point for unauthorized users.

Centralized Servers

Introduces a single point of failure on the network

Broadcast Network

Most vulnerable to address resolution protocol (ARP) or media access control (MAC)
address spoofing by both outside intruders and unauthorized users on local hosts.

Threats to Server Security

Unused service and ports

A common occurrence among system administrators is to install the operating system without paying
attention to what programs are actually being installed.

Unpathced Services

There is no such thing as perfect software and there is always room for further refinement.

Threats to Workstation and Home PC Security

Bad Passwords

Bad passwords are one of the easiest ways for an attacker to gain access to a system.

Vulnerable Client Application

Although an administrator may have a fully secure and patched server, that does not mean remote users are secure when accessing it.

Common Exploits and Attacks

Null or Default Passwords

Leaving administrative passwords blank or using a default password set by the product vendor.

Default Shared Keys

Secure services sometimes package default security keys for development or evaluation testing purposes.

Common Exploits and Attacks Contd...

IP Spoofing

A remote machine acts as a node on your local network, finds vulnerabilities with your servers, and installs a backdoor program or trojan horse to gain control over your network resources.

Eavesdropping

Collecting data that passes between two active nodes on a network by eavesdropping on the connection between the two nodes.

Common Exploits and Attacks Contd...

Service Vulnerabilities

An attacker finds a flaw or loophole in a service run over the Interne

Application Vulnerabilities

Attackers find faults in desktop and workstation applications

Denial of Service (DoS) Attacks

Attacker or group of attackers coordinate against an organization's network or server resources by sending unauthorized packets to the target host

MAY 18-20, 2012

Verifying Signed Packages

MAY 18-20, 2012

Install Signed Packages

MAY 18-20, 2012

BIOS and Boot Loader Security

BIOS passwords

1. Preventing Changes to BIOS Settings
2. Preventing System Booting

Securing non-X86 Platforms

Ex. Intel® ItaniumTM computers use the Extensible Firmware Interface (EFI) shell

MAY 18-20, 2012

Boot Loader Security

Boot Loader passwords

1. Preventing Access to Single User Mode

2. Preventing Access to the GRUB Console

3. Preventing Access to Insecure Operating Systems

Password Security

- Primary method that Fedora uses to verify a user's identity
- Data Encryption Standard (DES) and Message-Digest Algorithm (MD5)
- /etc/shadow and /etc/passwd

Creating Strong Passwords

- Do Not Use Only Words or Numbers
- Do Not Use Recognizable Words
- Do Not Use Words in Foreign Languages
- Do Not Use Personal Information
- Do Not Use Hacker Terminology (LEET)
- Do Not Invert Recognizable Words
- Do Not Write Down Your Password
- Do Not Use the Same Password For All Machines
- Make the Password at Least Eight Characters Long
- Mix Upper and Lower Case Letters
- Include Non-Alphanumeric Characters
- Pick a Password You Can Remember

MAY 18-20, 2012

Secure Password Creation Methodology

MAY 18-20, 2012

Creating User Passwords within an Organization

MAY 18-20, 2012

Forcing Strong Passwords

MAY 18-20, 2012

Password Aging

Disabling Root SSH Logins

MAY 18-20, 2012

The su Command

MAY 18-20, 2012

The sudo Command

MAY 18-20, 2012